CCIE Professional Development

Network Security Technologies and Solutions

A comprehensive, all-in-one reference for Cisco network security

ciscopress.com

Yusuf Bhaiji, CCIE No. 9305

CCIE Professional Development

Network Security Technologies and Solutions

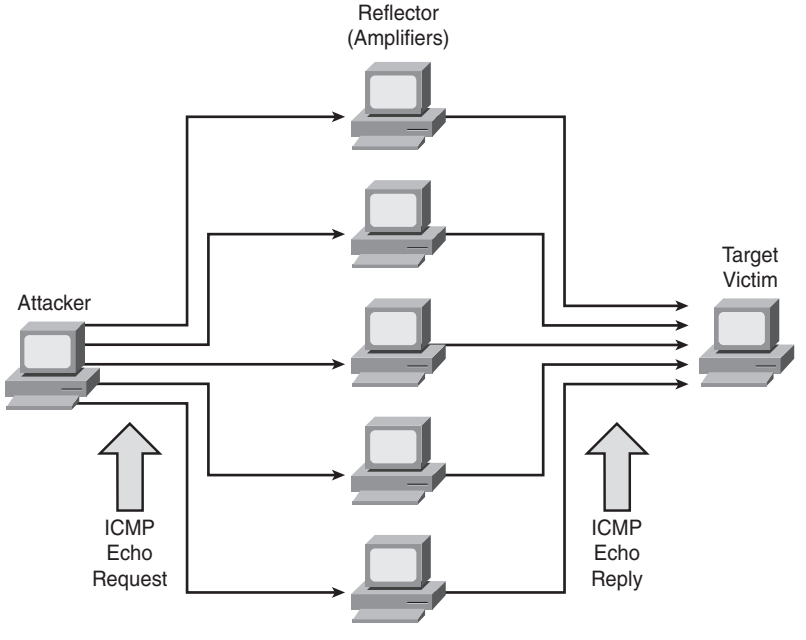
Yusuf Bhaiji, CCIE No. 9305

Cisco Press

Cisco Press
201 West 103rd Street
Indianapolis, IN 46290 USA

echo packet, they respond with an ICMP echo-reply packet to the victim address, thereby causing an ICMP flood situation.

Figure 7-1 *Smurf Attack*



Example 7-1 shows an extended access list with permit statements to identify smurf or fraggle attacks.

Example 7-1 *Characterizing a Smurf Attack*

```
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
access-list 101 permit ip any any
!
interface <suspected interface>
ip access-group 101 in
```

NOTE Characterization ACLs do not filter out traffic; all the ACL entries are permit statements because the objective is to categorize the traffic.

As shown in Figure 7-1, two possible victims are affected in this attack and need to be identified accordingly:

- Possibility of being a smurf target victim
- Possibility of being a smurf reflector

Use the **show ip access-list** command to display the access-list packet match statistics to identify the potential threat.

The **show ip access-list** command output in Example 7-2 shows a large number of ICMP echo reply packets, which is an indication of a potential ICMP flood or smurf attack on the ultimate target victim rather than the reflector.

Example 7-2 *Output of Smurf Target Victim Attack*

```
Router# show ip access-list
Extended IP access list 101
   permit icmp any any echo (5 matches)
   permit icmp any any echo-reply (2198 matches)
   permit ip any any (11205 matches)
```

When the **show ip access-list** command output indicates a large number of ICMP echo requests instead of echo replies, as shown in Example 7-3, this indicates that the network is being used as a reflector (amplifier). The same output could also mean that the network is experiencing a simple ICMP ping flood, not a smurf. In either case, if the attack is successful, both the egress and the ingress interfaces will be experiencing congestion with large packet counts on the interface. Furthermore, because of the amplification factor, the egress side will be more overloaded than the ingress side.

Example 7-3 *Output of Smurf Reflector Attack*

```
Router# show ip access-list
Extended IP access list 101
   permit icmp any any echo (5432 matches)
   permit icmp any any echo-reply (2 matches)
   permit ip any any (1904 matches)
```

There are several ways to distinguish the smurf attack from the simple ping flood:

- Smurf packets are sent to a directed broadcast address, rather than to a unicast address, whereas ordinary ping floods almost always use unicast. This can be checked in the addresses with the **log-input** keyword on the appropriate access list entry.
- When experiencing a smurf reflector attack, a disproportionate number of output broadcasts in the **show interface** counters is displayed, and usually a disproportionate number of broadcasts are sent in the **show ip traffic** display. A standard ping flood does not increase the background broadcast traffic.
- When experiencing a smurf reflector attack, there is more outbound traffic toward the uplink, as compared to the inbound traffic from the uplink. In general, there are more output packets than input packets on the suspected interface.

When a smurf reflector is closer to the intruder than the ultimate target, it is much easier to trace the attack. ISPs need to be closely involved in tracing such attacks. However, in other situations, the reflector may not be closer to the attacker than the target. The target could be on your own subnet with the reflector on the other side of the network. (The broadcast address does not determine the unicast destination that has been spoofed.)

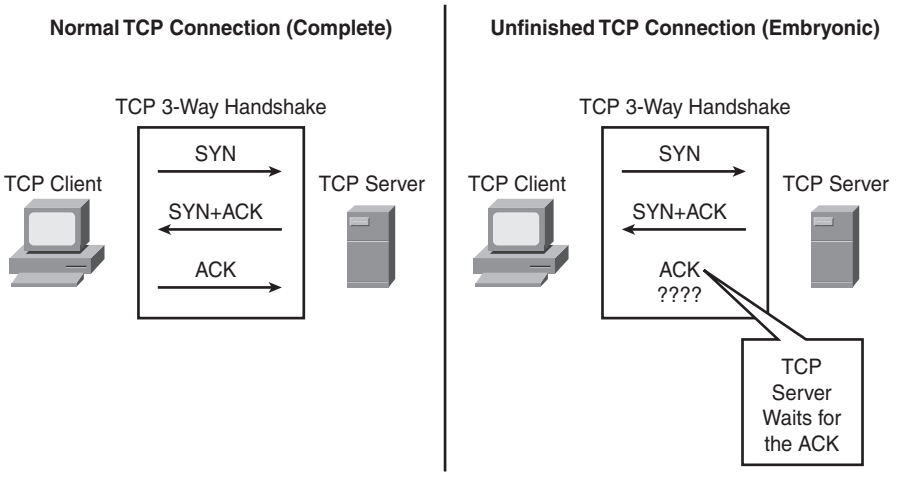
To stop Cisco routers from being reflectors in such attacks, use the **no ip directed-broadcast** interface configuration command. This should be configured on each interface of all routers. Note that **no ip directed-broadcast** is now the default on all interfaces, beginning with Cisco IOS Software Version 12.0. This command drops any packets on the router that are sent to a directed broadcast address that causes multiple hosts to respond to the ICMP echo request.

You can use several techniques to prevent or minimize the impact of smurf and similar ICMP flood attacks, such as rate-limiting (Committed Access Rate [CAR]), a filter using access lists, and Unicast Reverse Path Forwarding (uRPF) and IP Source Guard features, as discussed in the "IP Spoofing Attacks" section later in this chapter.

Using an ACL to Characterize SYN Attacks

There are many variations of SYN flood attacks, with the most common being a situation in which a target machine is flooded with TCP SYN connection requests. In most cases, the source addresses and source TCP ports of the connection request packets are randomized and spoofed. The objective is to force the target host to maintain TCP state information for a large number of incomplete connections (half-open connections), also called embryonic connections, which are illustrated in Figure 7-2.

Figure 7-2 *Unfinished Half-Open TCP Connection (Also Called Embryonic Connection)*



SYN flood attacks are sometimes easy to identify because the target host (such as the HTTP or SMTP server) becomes extremely slow, crashes, or hangs. SYN floods are not the only vector; several other vectors exist that are aimed in a similar flooding attack. Most people focus on SYN floods as a critical security attack vector. In reality, some SYN flood mitigation paths open the door for other TCP-based attack vectors.

TCP attack vectors are varied and include the following:

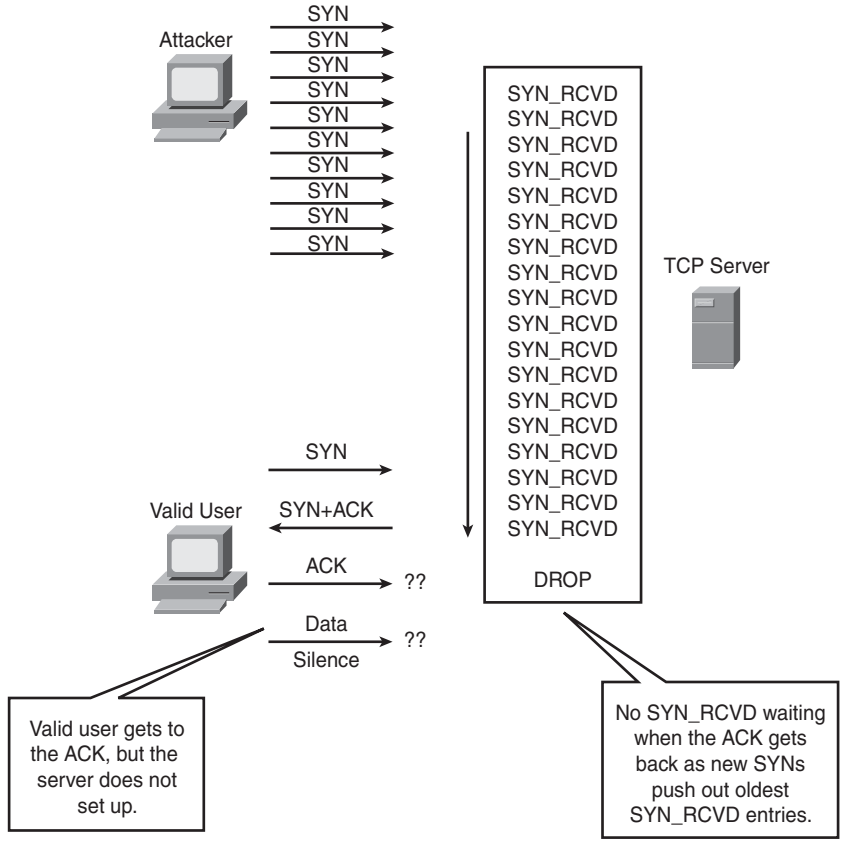
- SYN Flood
- ACK Flood
- SYN+ACK Flood
- SYN+RST Flood
- RST Flood
- Established Flood
- FIN Flood
- TCP Options Flood
- X-Tree Flood

There are two major types of SYN-flood attacks:

- **Nonspoofed source addresses:** Easy to trace, usually launched from compromised hosts (user workstations, servers, and the like)
- **Spoofed source addresses:** Difficult to trace, when spoofing invalid addresses from Bogon space (unallocated address range) or valid addresses from someone else's address blocks

SYN Round Trip Time (RTT) is the interval between the sending of SYN+ACK and reception of the corresponding ACK from the other host (receiver). A successful SYN flood occurs when the number of simultaneous SYNs exceeds the capacity of the victim's TCP Listen queue *and* the rate of SYNs exceeds the victim's ability to clear the SYN_RCVDs in an interval less than the SYN+ACK RTT. The objective of the attack is to crowd out valid SYN_RCVDs before the client's ACK has a chance to get to the server. If an ACK is received, and there is no available SYN_RCVD waiting, the connection fails and the DoS is successful, as depicted in Figure 7-3.

Figure 7-3 *SYN Flooding*



In summary, to successfully SYN-flood, the attacker must achieve the following:

- Fill and overflow the TCP server's memory so that the oldest SYN_RVCD entries are flushed.
- Fill the TCP queue faster than the typical SYN+ACK RTT so that valid customer SYN_RVCD entries are crowded out.

Example 7-4 shows an extended access list with permit statements to identify a TCP SYN attack. The TCP permit statement has several other options, such as matching FIN, URG, RST flags or established connections, or checking fragment packets.

Example 7-4 *Characterizing a TCP SYN Attack*

```
access-list 101 permit tcp any any syn
access-list 101 permit ip any any
!
interface <suspected interface>
ip access-group 101 in
```

Use the **show ip access-list** command to display the access-list packet match statistics to identify the SYN attack.

The output in Example 7-5 shows a large number of TCP SYN packets, an indication of a potential SYN flood to a target victim. The only nonattack condition that creates this signature is a massive overload of genuine TCP connection requests.

Example 7-5 *Output of Smurf Target Victim Attack*

```
Router# show ip access-list
Extended IP access list 101
    permit tcp any any syn (13174 matches)
    permit ip any any (438 matches)
```

Many features are available that you can use to reduce the impact of SYN floods. The effectiveness of these features depends on the environment; therefore, you should carefully examine these solutions. Some techniques available to prevent or minimize the impact of SYN flood attacks include the following:

- Rate-limiting (CAR).
- Context-Based Access Control (CBAC).
- TCP Intercept.
- On security appliances such as PIX firewalls, static and nat commands provide an option to monitor and control half-open embryonic connections. For more details, refer to static command in PIX documentation.
- Antispoofing: Do not allow traffic claiming to be sourced from customer IP blocks to ingress from the uplink or Internet.
- Anti-bogon: Do not allow traffic claiming to be sourced from reserved addresses or from an IPv4 block that has yet to be allocated by the Internet Assigned Numbers Authority (IANA).
- A source-based remote triggered black hole (RTBH) filtering technique can also be used as a SYN flood mitigation tool. This feature provides real-time defense against DDoS attacks by using a combination of IP routing features. To learn more about this technique, refer to the following white paper: www.cisco.com/warp/public/732/Tech/security/docs/blackhole.pdf.